

POLÍTICAS INTERNAS DE CIBERSEGURIDAD PARA LA AGENCIA DE TRANSFORMACIÓN DIGITAL



ÍNDICE

POLÍTICAS INTERNAS DE CIBERSEGURIDAD PARA AGENCIA DE TRANSFORMACIÓN DIGITAL.....	1
ÍNDICE.....	1
PRESENTACIÓN.....	3
MARCO NORMATIVO.....	4
GENERALES.....	5
GLOSARIO DE TÉRMINOS.....	6
RESPONSABILIDADES GENERALES.....	8
DEL TITULAR DE LA ATD.....	8
DE LA DIRECCIÓN DE GOBIERNO DIGITAL.....	8
DEL DEPARTAMENTO DE CIBERSEGURIDAD.....	8
DE LOS COLABORADORES.....	9
DE LAS RESPONSABILIDADES ADMINISTRATIVAS.....	9
DE LOS PROVEEDORES O TERCEROS.....	9
POLÍTICAS DE CIBERSEGURIDAD.....	10
Política de control de acceso.....	10
Política de gestión de contraseñas.....	11
Política de uso de recursos tecnológicos.....	12
Política de limpieza del puesto de trabajo.....	12
Política de software no autorizado.....	13
Política de descarga de ficheros (red externa/interna).....	13
Política de intercambio de información con otras organizaciones.....	13
Política de uso de los servicios de mensajería instantánea.....	14
Política de Gestión de Vulnerabilidades y Actualizaciones.....	14
Política de Respaldo y Continuidad de la Información.....	14
Política de Respuesta a Incidentes de Ciberseguridad y Concientización.....	16
Política de Seguridad en el Desarrollo y Adquisición de Software.....	16
Política de Relación con Proveedores y Terceros.....	16
Política de Seguridad Física.....	17
Política de Seguridad en Redes y Telecomunicaciones.....	17
Política de trabajo a distancia.....	18
Política de uso responsable de Inteligencia Artificial.....	19
ANEXOS.....	20



PRESENTACIÓN

La protección, confidencialidad, integridad y disponibilidad de la información, administrada o procesada por la Agencia de Transformación Digital del Estado de Quintana Roo constituye una responsabilidad para todo el personal servidor público, prestadores de servicios profesionales, proveedores y terceros que intervengan en la operatividad de la institución.

Para garantizar un entorno tecnológico resiliente y alineado con los estándares vigentes de gestión de riesgos informáticos, el Departamento de Ciberseguridad asumirá la responsabilidad de establecer las acciones en la materia. En este sentido, el departamento de ciberseguridad será el encargado de formular las políticas internas, promover mecanismos e infraestructura de protección tecnológica, fomentar el cumplimiento de las disposiciones normativas y promover una cultura de prevención mediante la capacitación y concientización en materia de ciberseguridad.



MARCO NORMATIVO

Constitución Política de los Estados Unidos Mexicanos.

Esta guía establece las políticas de ciberseguridad en la Agencia de Transformación Digital, en seguimiento al derecho a la protección de los datos personales y como parte de los esfuerzos de la ATD para fortalecer las capacidades tecnológicas públicas en apego al Artículo 16, párrafo II y el Artículo 25 , último párrafo de la Constitución Política de los Estados Unidos Mexicanos.

Ley Nacional para Eliminar Trámites Burocráticos.

La Ley Nacional para Eliminar Trámites Burocráticos, establece en su artículo 6, fracción XIII a la ciberseguridad como uno de los principios que deben observar los Sujetos Obligados en el cumplimiento de sus obligaciones en materia de simplificación administrativa, digitalización de trámites y servicios y fortalecimiento de capacidades tecnológicas públicas. Asimismo, el artículo 25, fracciones V y VI, prevé la observancia de estándares de seguridad y mecanismos de actualización tecnológica para la digitalización de trámites y servicios.

La presente política se emite en cumplimiento a las atribuciones conferidas en el Artículo 13, fracción XVII, como apoyo y acompañamiento a los Sujetos Obligados en la recepción, implementación y actualización de las soluciones tecnológicas, siguiendo el principio de ciberseguridad establecido en la ley.

Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Quintana Roo.

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados, define la obligación del Estado por garantizar la privacidad de los individuos y velar por que no se incurran en conductas que afecten arbitrariamente a los individuos con su información como lo menciona en el Artículo 8 de la Ley.

Con el objetivo de proteger los datos personales de los individuos, se emiten las políticas para la protección del ecosistema de Tecnologías de los Sujetos Obligados de la Administración Pública Estatal como medida preventiva.

Plan Estatal de Desarrollo 2023-2027.

El Plan Estatal de Desarrollo 2023 - 2027 es un documento que define las prioridades del Estado para cubrir las necesidades de la ciudadanía. En el tema 5.24 Transparencia y Combate a la Corrupción, en la línea de acción 5.24.3.7 se especifica

"Promover la ciberseguridad al interior de las diferentes instancias gubernamentales del Estado mediante la promoción de políticas, mecanismos de prevención y protocolos de respuesta ante incidentes digitales y cibernéticos."

Decreto de Creación de la Agencia de Transformación Digital.

La Agencia de Transformación Digital del Estado de Quintana Roo, como Autoridad Estatal de Simplificación y Digitalización, cuenta con la facultad para diseñar e implementar políticas públicas en materia TIC, establecer políticas y lineamientos para la gestión y administración de los Centros de Datos de los Sujetos Obligados y proponer lineamientos y estándares, para fortalecer, modernizar y armonizar los sistemas tecnológicos de la Administración Pública Estatal, como se establece en el Artículo 6, sección II, V y VI.



GENERALES

El presente documento se elaboró con base en los principios, lineamientos y buenas prácticas de ciberseguridad establecidos en la "Guía de Ciberseguridad de la Agencia de Transformación Digital para la Administración Pública Estatal", publicado en la página oficial, en el apartado de Ciberseguridad, accesible en la url: <https://atd.qroo.gob.mx/ciberseguridad/>.

Estas disposiciones son de aplicación general y observancia obligatoria para:

- Todo el personal que preste sus servicios a la ATD, sin importar su régimen de contratación, servidores públicos de confianza, de base, personal por honorarios, etc.
- Proveedores, contratistas, consultores externos y terceros que, por la naturaleza de sus funciones o contratos, requieran interactuar, administrar o tener acceso al ecosistema tecnológico de la ATD.

GLOSARIO DE TÉRMINOS

ATD: Agencia de Transformación Digital del Estado de Quintana Roo.

Autenticación Multifactor (MFA): Método de control de acceso que requiere que el usuario presente al menos dos evidencias diferentes para verificar su identidad antes de otorgar acceso.

Cifrado: Proceso técnico mediante el cual los datos se vuelven ilegibles para personas no autorizadas utilizando algoritmos seguros.

Contraseñas robustas: Son aquellas diseñadas para que sean difíciles de adivinar o descifrar.

Crackeado: La acción de vulnerar sistemas o descifrar contraseñas con fines maliciosos o delictivos.

Ecosistema Tecnológico: Conjunto integrado de redes, servidores, estaciones de trabajo, plataformas de software, bases de datos y servicios en la nube utilizados por la ATD.

Fichero: Un conjunto de datos almacenados en un dispositivo.

Mensajería Instantánea: Se entiende por mensajería instantánea, cualquier aplicación que permite conversaciones o comunicaciones en tiempo real.

Mínimo Privilegio: Principio de seguridad que establece que a un usuario se le deben otorgar únicamente los accesos estrictamente necesarios para desempeñar sus funciones laborales.

Software No Autorizado: Cualquier programa informático, aplicación, extensión o código que no cuente con una licencia institucional vigente o que no haya sido validado y aprobado formalmente por el área de Tecnologías y/o Ciberseguridad de la ATD.

TIC: Tecnologías de Información y Comunicación.

Usuarios críticos: son usuarios esenciales para la continuidad operativa y la protección de datos sensibles de una organización.

Usuarios privilegiados: Son las credenciales de acceso que otorgan permisos elevados para interactuar con esas cuentas críticas.

VPN (Virtual Private Network): Tecnología que permite establecer una conexión segura y cifrada a una red de manera remota.

SFTP (Secure File Transfer Protocol): Protocolo seguro para transferir archivos mediante una conexión cifrada.

Zero Trust: Modelo de seguridad que verifica y autoriza cada acceso, sin asumir confianza por ubicación o usuario.

Trazabilidad: Es la capacidad de registrar, identificar y rastrear el estado, la ubicación y el historial de servicios o interacciones a lo largo de los procesos operativos.

RESPONSABILIDADES GENERALES

DEL TITULAR DE LA ATD

1. El titular puede expedir, abrogar, derogar o autorizar reformas y adiciones a las políticas Internas de Ciberseguridad.
2. Gestionar y autorizar, conforme a la disponibilidad presupuestal, la suficiencia de recursos financieros, materiales y humanos para el cumplimiento de la política de ciberseguridad..
3. Instruir la correcta implementación de los controles técnicos establecidos en este documento.
4. Instruir la difusión y la observancia obligatoria con los Coordinadores y Directores de las áreas, quienes a su vez deberán socializar con el personal de la ATD las políticas descritas en el presente documento.

DE LA DIRECCIÓN DE GOBIERNO DIGITAL

1. Coadyuvar, dentro del ámbito de sus atribuciones, en la implementación de los controles técnicos de ciberseguridad definidos por el Departamento de Ciberseguridad, cuando éstos correspondan a la administración del ecosistema tecnológico de la ATD.
2. Registrar las evidencias necesarias para sustentar cualquier anomalía técnica o de seguridad que se presente en el ecosistema tecnológico de la ATD, dentro del ámbito de sus atribuciones y capacidades técnicas, en coordinación con el Departamento de Ciberseguridad.
3. Atender las incidencias que se presenten en el ecosistema tecnológico de la Agencia de Transformación Digital, como administrador del mismo.
4. Solicitar los recursos económicos, tecnológicos, físicos y humanos necesarios para la correcta aplicación de las políticas establecidas en el presente documento.
5. Mantener un control de registros de alta, modificación o baja de usuarios utilizando el "FORMATO DE SOLICITUD DE USUARIOS (ALTA, BAJA Y CAMBIO)" incluido en los anexos del presente documento.
6. Entregar los usuarios de manera personal, al responsable en sobre cerrado e impreso utilizando el "FORTMATO DE ENTREGA DE USUARIOS" incluido en los anexos del presente documento.
7. Realizar, en coordinación con el Departamento de Ciberseguridad, el monitoreo técnico del uso de las páginas de internet y aplicaciones de mensajería instantánea autorizadas, conforme a los controles y criterios de

**DIRECCIÓN DE TRANSFORMACIÓN Y AGENDA DIGITAL
DEPARTAMENTO DE CIBERSEGURIDAD**

seguridad establecidos, a fin de detectar actividades no autorizadas, comportamientos anómalos o posibles abusos de los privilegios asignados.

DEL DEPARTAMENTO DE CIBERSEGURIDAD

1. Proponer los mecanismos, políticas, lineamientos y/o buenas prácticas en ciberseguridad a la Dirección General para su validación y aprobación.
2. Actualizar las propuestas de manera integral al menos una vez al año, o bien, de manera extraordinaria cuando ocurran cambios mayores en la infraestructura tecnológica o se detecten nuevas amenazas de alto impacto.
3. Coadyuvar en el análisis de las incidencias a la Dirección de Gobierno Digital.
4. Coadyuvar en la implementación técnica de estas políticas en el ecosistema tecnológico de la ATD en coordinación con la Dirección de Gobierno Digital.
5. Participar en capacitaciones en materia de ciberseguridad con base en estas políticas, para el correcto entendimiento e implementación de los colaboradores de la ATD.
6. Promover el cumplimiento de las políticas establecidas en el presente documento a los servidores públicos de la ATD.
7. El área de ciberseguridad, tendrá la facultad de implementar las medidas necesarias para la correcta implementación de estas políticas con la autorización del Director General.
8. El departamento de Ciberseguridad, puede establecer nuevas políticas, y actualizar el presente documento con la autorización del Director General y que será aplicable de manera inmediata posterior a su publicación en la página oficial de la ATD.

DE LOS COLABORADORES

1. Conocer, comprender y cumplir con cada una de las políticas descritas en este documento.
2. Reportar de manera inmediata, por medio del correo electrónico institucional, al Departamento de Ciberseguridad cualquier anomalía, vulnerabilidad o evento que pudiera representar un riesgo para la seguridad de la información o del ecosistema tecnológico de la ATD, con copia a la Dirección de Gobierno Digital.

[Handwritten signatures and initials in blue ink]

DE LAS RESPONSABILIDADES ADMINISTRATIVAS

1. Aplicar en caso incumplimiento de las obligaciones establecidas en los presentes lineamientos por parte de las personas servidoras públicas la sanción de conformidad con lo establecido en la Ley General de Responsabilidades Administrativas y demás normatividad aplicable.
2. Asegurar que todo el personal que preste sus servicios a la ATD, firme el "Formato de aceptación de políticas de ciberseguridad de la ATD" al ingreso de los servidores públicos a laborar con la agencia y en cada actualización o cambio en las políticas internas de ciberseguridad.

DE LOS PROVEEDORES O TERCEROS

1. Conocer, comprender y cumplir con cada una de las políticas descritas en este documento.
2. Firmar la carta de confidencialidad expedida por la ATD, previo al inicio de labores o actividades que puedan involucrar información privada o sensible perteneciente a la ATD.

POLÍTICAS DE CIBERSEGURIDAD

Política de control de acceso.

El control de acceso al ecosistema de TIC , deberán de contar con gestión por roles o perfiles, dependiendo del tipo de usuario y los permisos según el rol que requiera desempeñar.

1. Todos los usuarios del ecosistema tecnológico deberán contar con información de identificación única e inequívoca.
2. Todos los usuarios deberán contar con un perfil o rol de acceso asignado conforme a las funciones y responsabilidades inherentes a su puesto o actividad.
3. El acceso a sistemas, aplicaciones, plataformas, bases de datos y recursos tecnológicos deberá apegarse al modelo de Identidad y Accesos (IAM), basado en el *Eje 5: Identidad, accesos y Zero Trust* en la "Guía de Ciberseguridad para la Administración Pública Estatal" de la ATD.
4. Queda prohibido el uso de cuentas genéricas, compartidas o anónimas, sin excepción alguna bajo el modelo Zero Trust definido en la "Guía de Ciberseguridad para la Administración Pública Estatal" de la ATD.
5. Toda alta, modificación o baja de accesos deberá ser autorizada por el responsable del área correspondiente.
6. Los accesos privilegiados o administrativos deberán ser controlados, monitoreados y asignados únicamente por el personal de la Dirección de Gobierno Digital.
7. Las cuentas de usuario deberán deshabilitarse inmediatamente cuando exista terminación de la relación laboral, cambio de funciones o detección de uso indebido.
8. Los accesos a información clasificada, sensible o confidencial deberán contar con mecanismos adicionales de autenticación y trazabilidad.
9. En caso de existir accesos remotos, estos deberán realizarse mediante mecanismos seguros de autenticación multifactor (MFA) y canales cifrados.
10. Toda alta, baja o modificación de acceso deberá solicitarse mediante el formato autorizado.
11. La asignación de permisos deberá apegarse a una matriz de roles/perfiles y al principio de mínimo privilegio.
12. La Dirección de Gobierno Digital y el Departamento de Ciberseguridad deberán mantener los registros de altas, modificaciones y bajas de accesos, de acuerdo con el ámbito de sus respectivas atribuciones.

Política de gestión de contraseñas.

Esta política tiene como objetivo establecer los criterios mínimos de seguridad para la creación, administración y protección de contraseñas institucionales.

1. Todos los usuarios deberán utilizar contraseñas robustas y únicas.
2. Las contraseñas deberán cambiarse a una personalizada, inmediatamente después del primer inicio de sesión.
3. Las contraseñas deberán contener una longitud mínima de 12 caracteres y combinar letras mayúsculas, minúsculas, números y caracteres especiales.
4. Queda prohibido compartir contraseñas entre usuarios, áreas, proveedores o terceros.
5. Las contraseñas no deberán almacenarse en texto plano ni anotarse en lugares visibles.
6. Todos los usuarios críticos y usuarios privilegiados deberán utilizar autenticación multifactor (MFA) para iniciar sesión toda vez que sea necesario..
7. Las contraseñas deberán cambiarse inmediatamente en caso de sospecha de compromiso.
8. La reutilización de contraseñas anteriores deberá restringirse técnicamente.
9. Queda prohibido utilizar datos personales del usuario como: nombre, apellidos, fecha de cumpleaños, fragmentos del correo electrónico registrado, entre otros que pudieran ser predecibles.
10. Los sistemas deberán bloquear los intentos fallidos de autenticación con un límite máximo de 3 intentos.
11. El restablecimiento de contraseñas deberá realizarse por medio de una solicitud formal desde el formato de modificación o actualización de usuarios.



Política de uso de recursos tecnológicos.

Regular el uso adecuado de los recursos tecnológicos institucionales para preservar la confidencialidad, integridad y disponibilidad de la información.

1. Los recursos tecnológicos deberán utilizarse exclusivamente para fines laborales o institucionales autorizados.
2. Queda estrictamente prohibida la instalación de software, extensiones de navegador o herramientas de terceros que no cuenten con la licencia correspondiente o la autorización expresa del área de TI o Ciberseguridad.
3. Los usuarios deberán abstenerse de realizar actividades que comprometan la seguridad de la infraestructura tecnológica institucional.
4. El uso de dispositivos personales para actividades institucionales deberá sujetarse a controles de seguridad establecidos por la organización.
5. La Jefatura de Ciberseguridad podrá definir controles técnicos para bloquear el acceso a sitios web de alto riesgo (sitios de apuestas, contenido para adultos, descargas ilegales, plataformas de almacenamiento no autorizadas ,etc).
6. Los usuarios reconocen que el tráfico de red, los correos institucionales y las actividades en equipos oficiales están sujetos a monitoreo y auditoría por seguridad, respetando los límites legales de privacidad.
7. Todo traslado, préstamo, baja, sustitución o reasignación de equipo tecnológico deberá registrarse en el inventario institucional y contar con evidencia de entrega-recepción.

Política de limpieza del puesto de trabajo.

Esta política tiene como objetivo mantener los puestos de trabajo libres de obstáculos que puedan dañar los bienes inmuebles de la institución.

1. Mantener limpio el puesto de trabajo en todo momento, libre de basura, alimentos, bebidas y dispositivos que no pertenezcan a la ATD o que puedan causar distracción de sus labores.
2. Queda prohibido comer en áreas de trabajo, como escritorios, pasillos, oficinas o salas de juntas.
3. Deberá trabajar de manera ordenada evitando mantener cosas que no serán utilizadas sobre el puesto de trabajo
4. Deberá evitar tener información de sus labores. documentos, trabajos, información personal, en el escritorio de sus equipos, al momento de abandonar o retirarse momentáneamente de su puesto de trabajo.

Política de software no autorizado.

La presente política se establece para definir el uso correcto del software de la empresa o en su caso, aquello que haya sido adquirido para los fines correspondientes a sus labores.

1. El uso de software no autorizado queda prohibido en los equipos de cómputo asignados o que se encuentren conectados a la infraestructura tecnológica de la ATD.
2. La Dirección de Gobierno Digital, puede restringir los permisos para instalar software no permitido por esta política.
3. Está prohibido la instalación de software crackeado en los equipos pertenecientes a la ATD y/o conectados a la red de telecomunicaciones (WiFi o por cable).
4. Se permite el uso de software libre, sin embargo, este deberá pasar por previa autorización por el Departamento de Ciberseguridad y la Dirección de Gobierno Digital.

Política de descarga de ficheros (red externa/interna).

1. Ficheros, documentos, software, etc, pertenecientes a la ATD y/o servidores públicos (derivados de sus funciones laborales), se pueden compartir únicamente por medios oficiales, correo electrónico, chat oficial de la ATD y/o por medio de un servidor de SFTP.
2. Queda prohibido la descarga de cualquier tipo de fichero perteneciente a páginas no oficiales.
3. Queda prohibido la descarga de software perteneciente a sitios de descarga de contenido, software crackeado, VPN no oficial, etc.

Política de intercambio de información con otras organizaciones.

1. Para el intercambio de información con otras Instancias Gubernamentales, deberá ser por medio de SSH con protocolos de SFTP en archivos o ficheros y por el medio autorizado por el área responsable de la seguridad de la información de la ATD
2. Se deberá de firmar un acuerdo de confidencialidad en caso de ser necesario dependiendo del tipo de información que se requiera compartir.
3. Solo los documentos que se pretenden compartir, deberán de poder acceder con un usuario y/o contraseña en plataformas legítimas o autorizadas.



4. El intercambio de información mediante APIs deberá realizarse a través de mecanismos seguros de autenticación, autorización y cifrado, garantizando la confidencialidad, integridad y disponibilidad de la información intercambiada.

Política de uso de los servicios de mensajería instantánea.

1. Se permite el uso de mensajería instantánea únicamente por medios oficiales autorizados por el titular de la ATD.
2. La comunicación deberá ser por medio del correo electrónico institucional y los medios autorizados por el titular de la ATD.
3. Evitar el uso de estos canales para transmitir datos personales sensibles o información confidencial, prefiriendo canales formales para ese fin.

Política de Gestión de Vulnerabilidades y Actualizaciones.

1. Los sistemas operativos de servidores, estaciones de trabajo y dispositivos de red deberán contar con parches de seguridad aplicados en un plazo no mayor a 5 días naturales tras su liberación por el proveedor para vulnerabilidades catalogadas como "Altas".
2. Para vulnerabilidades catalogadas como "Críticas", deberán ser aplicados en un plazo no mayor a 72 horas.
3. Se deberán realizar análisis de vulnerabilidades (escaneos internos y externos) con una periodicidad mínima mensual, y pruebas de penetración al menos una vez al año o posterior a modificaciones mayores en la infraestructura.
4. Queda prohibido el uso de sistemas operativos o software que hayan alcanzado el fin de su ciclo de vida y no reciban actualizaciones de seguridad del fabricante.
5. Se prohíbe la descarga de información y/o archivos que no tengan relación directa con la ATD o con las funciones propias del cargo.

Política de Respaldo y Continuidad de la Información.

1. Los sistemas críticos de la institución (bases de datos ciudadanas, sistemas financieros, trámites en línea) deberán contar con respaldos automatizados diarios que serán removidos al año de su resguardo, en caso de que ya no sean requeridos para alguna consulta.
2. La información operativa general (no crítica) se respaldará semanalmente en discos duros externos, que no se encuentren activos y fuera de la red institucional, bajo resguardo y en un lugar seguro para mantener la integridad de la información.

3. Se deberán mantener al menos dos copias de los datos, almacenadas en dos tipos de medios distintos, con una de las copias resguardada en una ubicación física o nube externa y lógicamente aislada de la red principal.
4. Se deberán realizar simulacros semestrales de restauración de respaldos para validar la integridad de los datos y asegurar el cumplimiento de los tiempos de recuperación definidos por la institución.

Política de Respuesta a Incidentes de Ciberseguridad y Concientización.

1. Toda persona servidora pública o colaborador que sospeche o detecte un evento anómalo, deberá reportarlo inmediatamente al área de ciberseguridad que a su vez trabajará de manera coordinada con la Dirección de Gobierno Digital para mitigar cualquier eventualidad que ponga en riesgo la seguridad de la información.
2. Todo el personal de la institución deberá cursar de manera obligatoria al menos una capacitación anual en materia de ciberseguridad, concientización y protección de datos personales.
3. La institución mantendrá un Plan de Respuesta a Incidentes actualizado que defina roles, canales de comunicación y flujos de contención para amenazas críticas como ransomware, fuga de datos o denegación de servicio.

Política de Seguridad en el Desarrollo y Adquisición de Software.

1. Todo nuevo proyecto de desarrollo de software debe integrar requisitos de seguridad y privacidad desde la fase de planeación.
2. Antes de pasar cualquier sistema o actualización al entorno de producción, el código debe someterse a análisis estáticos y dinámicos para detectar vulnerabilidades.
3. Se deben mantener ambientes técnica y lógicamente independientes para Desarrollo, Pruebas y Producción.
4. Queda estrictamente prohibido utilizar datos reales de ciudadanos o bases de datos de producción en los entornos de desarrollo o pruebas.
5. Todo software adquirido o contratado bajo la modalidad de Software como Servicio debe acreditar certificaciones de seguridad (como ISO 27001 o SOC 2) y auditorías vigentes antes de su integración con la infraestructura institucional.

[Handwritten signatures and initials in blue ink]

Política de Relación con Proveedores y Terceros.

1. Ningún proveedor podrá iniciar operaciones o tener acceso a las instalaciones, sistemas o información de la institución sin haber firmado previamente un Convenio de Confidencialidad y No Divulgación.
2. Los contratos de adquisición de bienes o servicios tecnológicos deben incluir penalizaciones explícitas por incumplimiento de medidas de seguridad
3. Los contratos de adquisición de bienes o servicios tecnológicos deben incluir la obligación de notificar cualquier brecha de seguridad.
4. Todo proveedor deberá de estar inscrito en el padrón de proveedores del Estado de Quintana Roo.
5. Al finalizar la relación laboral, deberán de realizar el proceso de baja de usuarios establecido en la ATD.

Política de Seguridad Física.

1. Las áreas donde se almacena información sensible o infraestructura crítica deben contar con barreras físicas, control de acceso biométrico o por tarjeta magnética, y registro con bitácora de entradas y salidas.
2. Al retirarse de su puesto de trabajo, el personal debe bloquear su sesión de cómputo y resguardar bajo llave cualquier documento físico que contenga datos personales, financieros o información reservada.
3. Los centros de datos, cuartos de telecomunicaciones, cuartos de servidores o similares, deben ser monitoreados mediante sistemas de Circuito Cerrado de Televisión.
4. Las grabaciones deben mantenerse en resguardo para su consulta por un periodo mínimo de 30 a 90 días conforme a la normativa de protección de datos personales.
5. Los centros de datos, cuartos de telecomunicaciones, cuartos de servidores o similares, deberán contar con sistemas de UPS para el respaldo de la energía eléctrica en caso de cortes de servicio energético por mantenimiento o corrección de fallos.
6. Los centros de datos, cuartos de telecomunicaciones, cuartos de servidores o similares, deberán contar con sistemas contra incendios por gas inundante, los cuales deben recibir mantenimiento preventivo trimestral con enfoque en la continuidad del servicio.
7. Las personas visitantes, proveedoras o externas deberán registrarse y permanecer acompañadas en todo momento por personal autorizado cuando ingresen a áreas críticas como el centro de datos, site de telecomunicaciones o site de servidores.

Política de Seguridad en Redes y Telecomunicaciones.

1. La red institucional debe estar segmentada mediante firewalls de nueva generación
2. La red institucional deberá contar con Redes de Área Local Virtual (VLAN) separadas para servidores, computadoras, dispositivos IoT/CCTV y una red aislada para visitantes.
3. Toda información gubernamental sensible o datos personales que se transmitan a través de redes públicas o internas deben ser cifrados utilizando protocolos seguros y vigentes (TLS 1.3 en servicios web, SSH para conexiones remotas)
4. Queda estrictamente prohibido el uso de protocolos obsoletos e inseguros como HTTP o Telnet, implementando protocolos seguros como HTTPS y TLS o SSH para conexiones remotas.
5. Las redes de WiFi oficiales para el personal deben de utilizar autenticación robusta y segura.
6. Se deberán de implementar y mantener activos sistemas de detección y respuesta en dispositivos finales, (EDR) y/o detección y respuesta extendida en dispositivos finales, (EXDR), para la detección de intrusos en los perímetros de la red y para identificar patrones de tráfico malicioso.
7. Las comunicaciones institucionales de voz, videoconferencia, colaboración o transmisión en tiempo real deberán utilizar protocolos seguros, como SRTP, TLS u otros equivalentes vigentes.
8. Se deberá mantener diagramas de red, inventario de dispositivos, reglas de firewall, configuraciones críticas y certificados digitales relacionados con las comunicaciones institucionales como respaldo en caso de presentarse alguna contingencia.
9. Las reglas de firewall, segmentación, puertos publicados y servicios expuestos deberán revisarse al menos de forma semestral o cuando exista un cambio mayor en la infraestructura.
10. Queda prohibido habilitar accesos remotos, abrir puertos o modificar configuraciones de red sin autorización y registro técnico correspondiente.

Política de trabajo a distancia.

1. Queda estrictamente prohibido laborar en espacios públicos abiertos cuando se maneje información clasificada como Interna, Confidencial o Reservada.
2. Las conexiones remotas a los servicios tecnológicos institucionales como la administración de servidores, equipos de telecomunicaciones, bases de datos,

entre otros, deberá ser por medio de VPN con IPSec y conexiones seguras como SSH.

3. Queda estrictamente prohibido utilizar computadoras o tabletas personales para procesar, almacenar o transmitir información gubernamental.
4. Queda terminantemente prohibido conectar el equipo institucional a redes Wi-Fi públicas, abiertas o compartidas sin contraseña.
5. En caso de pérdida, robo del equipo de cómputo, sospecha de infección por malware o vulneración de la red doméstica, el servidor público deberá reportarlo inmediatamente a la Dirección de Gobierno Digital.

Política de uso responsable de la Inteligencia Artificial.

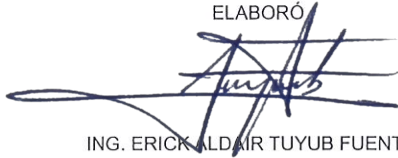
Esta política, plantea el uso responsable de la inteligencia artificial dentro de la ATD, siendo que, no se prohíbe su uso para la consulta de información y para agilizar procesos recurrentes, se plantea regular su uso para la protección de la información de la ATD.

1. Se prohíbe introducir información confidencial de la ATD , datos personales de colaboradores y/o usuarios externos que se almacenen o se tenga conocimiento para realizar consultas, analizar información, etc.
2. En caso de estar disponible, utilizar cuentas corporativas exclusivamente para realizar consultas a la IA siempre y cuando dichas consultas estén relacionadas con alguna información o labor de la ATD.
3. Se prohíbe el uso de las cuentas de IA corporativas para consultas con motivos personales. o ajenos a la ATD.
4. Todo contenido generado por la IA, debe considerarse una sugerencia, por lo que deberá ser revisado, validado y asumir la responsabilidad del trabajo elaborado.
5. Es fundamental citar correctamente el uso de IA y ser responsable sobre su uso, manteniendo la integridad profesional.

ANEXOS

1. FORMATO DE SOLICITUD DE USUARIOS (ALTA, BAJA Y CAMBIO)
2. FORMATO DE ENTREGA DE USUARIOS
3. FORMATO DE ACEPTACIÓN DE POLÍTICAS DE CIBERSEGURIDAD DE LA ATD
4. FORMATO DE REPORTE DE INCIDENTES

ELABORÓ



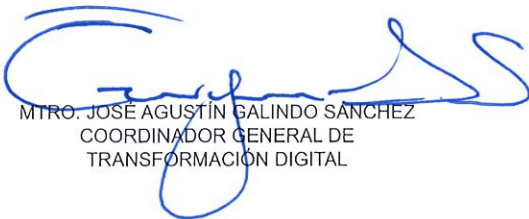
ING. ERICK ALDAIR TUYUB FUENTES
JEFE DE DEPARTAMENTO DE
CIBERSEGURIDAD

REVISÓ



ING. DULCE GABRIELA HERNÁNDEZ ESQUIVEL
DIRECTORA DE TRANSFORMACIÓN Y AGENDA
DIGITAL

VALIDÓ



MTRO. JOSÉ AGUSTÍN GALINDO SÁNCHEZ
COORDINADOR GENERAL DE
TRANSFORMACIÓN DIGITAL

AUTORIZÓ



M.E. JAVIER ABRAHAM AYUSO SÁNCHEZ
DIRECTOR GENERAL DE LA AGENCIA DE
TRANSFORMACIÓN DIGITAL